A Guide to Enterprise Risk Management

Richard P. Kusserow | March 2025

Key Points:

- **Goals, responsibility, assessment, and steps for mitigation**
- **Compliance should not have overall responsibility for ERM, only for a supporting role**

Enterprise Risk Management (ERM) is critical for any health care organization. In simple terms, it is a strategy that investigates and addresses all key risks to which an organization is vulnerable and involves coordinating risk management activities across all departments and operations. The goals of ERM are to prevent liabilities. This involves advancing safe and trusted healthcare, managing uncertainty, maximizing value protection and creation, encouraging multidisciplinary accountability, optimizing organizational readiness, promoting a positive organizational culture that will impact readiness and success, utilizing data/metrics to prioritize risks, and aligning risk appetite and strategies for avoiding costly consequences for non-compliance. For many organizations, determining who has overall responsibility for ERM is a problem. The recent 2024 Compliance Benchmark Survey found that thirty percent of reporting organizations stated the Compliance Officer as having primary responsibility for risk management. There is no question that the Compliance Officer should have responsibility for regulatory compliance-related risks but is not competent in addressing all organizational risk areas, including financial, medical, technical, and operational areas. The overall responsibility of ERM begins with the Board of Directors providing oversight of the overall risk management strategy and ensuring it aligns with the organization’s goals. Day-to-day implementation is typically managed by a dedicated risk management team including the CEO, COO, CFO, CIO, and other key leadership figures within the hospital. Often, they will assign an executive the responsibility for designing, implementing, and managing the ERM process, including establishing a framework for identifying, assessing, analyzing, monitoring, managing, and mitigating risks that could have an impact on the organization. Many organizations, especially hospitals, have a Chief Risk Officer assigned this responsibility.

Copyright © 2025 Strategic Management Services, LLC

ERM begins with a Risk Assessment that identifies risks that may affect operations, including financial planning and operations, clinical/patient safety, technical/cybersecurity, workforce safety/security, privacy/propriety protection, legal/regulatory compliance, etc. This is followed by identifying means and methods for ranking the levels of risk that enable setting priorities, strategies, and actions to mitigate exposure and impact on operations. Risk mitigation and management is the process to focus on: (a) ways a risk can impact the business; (b) likelihood and potential impact of a risk on a specific department or operation; (c) root cause for the risk; and (d) steps that can mitigate exposure. The impact of a risk can be loss of reputation, financial consequences, compliance failure, enforcement actions by regulatory authorities, health and safety of patients and staff endangerment, legal consequences, loss of revenue, cybersecurity attacks, and others. This can be reduced to metrics that set priorities for mitigation. The steps to follow in addressing ERM include the following:

1. Engage Board and Leadership. It is critical to a successful ERM program to engage the board and executive leadership in the process. This includes ensuring active involvement of program managers who are in a position to identify risks, as well as solutions, to risk within their areas of operational responsibility.
2. Risk Identification. Take time to identify all organizational risks, both external and internal, along with determining key risk factors, including operational, probability, financial, reputation, safety, quality of care, etc.
3. Rank Risks. After identifying risks, it is important to assess the level of vulnerability in terms of those that are likely to happen and their financial, reputational, and/or regulatory impact.
4. Risk Mitigation Plan. Decide on the priority for addressing identified risks. In most health care organizations, the number of risks is great and may require a multi-year plan that begins with those areas of highest risk level and works down the list.
5. Monitoring and Reporting. It is critical that once a risk area has been identified, it be included in a mitigation plan to address the risks. This includes monitoring and reporting to the party responsible for overseeing the entire process, who will ensure accountability for those responsible for risk mitigation.

For more information on this topic, contact Richard Kusserow (rkusserow@strategicm.com). You can also keep up-to-date with Strategic Management Services by following us on LinkedIn.

Copyright © 2025 Strategic Management Services, LLC

About the Author

Richard P. Kusserow established Strategic Management Services, LLC, after retiring from being the DHHS Inspector General, and has assisted over 2,000 health care organizations and entities in developing, implementing and assessing compliance programs.

Copyright © 2025 Strategic Management Services, LLC